

## UNITED STATES DISTRICT COURT

for the  
Western District of WashingtonIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
The Person of KUANG CHI WAN

Case No. MJ23-033

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The Person of KUANG CHI WAN, as described in Attachment A, incorporated herein by reference.  
located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2332g(a)-(c)	Missile Systems Designed to Destroy Aircraft

The application is based on these facts:

- ☒ See Affidavit of Special Agent Gary Phillips continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



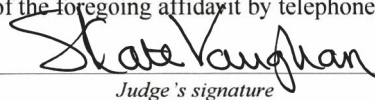
Applicant's signature

Gary Phillips, Special Agent, FBI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/20/2023



Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge

Printed name and title

**ATTACHMENT A**

**Person to Be Searched**

The property to be searched is the person of KUANG CHI WAN, also known as “James Wan,” and any bag, backpack, or luggage with him and all electronic devices, storage drives, and closed or locked containers found therein, including but not limited to a Huawei cell phone with Android ID 4497286113129079259 and serial number HWEML:BPN0218C05002044, and a PC laptop (the “Devices”).

This warrant authorizes the seizure of electronic devices as well as forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

**Property to be Seized**

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. §§ 2332g(a)(1)(A), 2332g(a)(1)(B), and 2332g(c)(1) (the “Subject Crimes”) and involve WAN since January 2019, including:

- a. Any communications in furtherance of the Subject Crimes, including but not limited to email and encrypted chat communications;
- b. Any location information regarding WAN or other coconspirators involving in the Subject Crimes;
- c. All documents regarding the Subject Crimes, including draft or finalized contracts and photographs; and
- d. All bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government,

1 attorney support staff, and technical experts. Pursuant to this warrant, the FBI may  
2 deliver a complete copy of the seized or copied electronic data to the custody and control  
3 of attorneys for the government and their support staff for their independent review.

4 During the execution of the search of any Apple brand device(s) (such as an  
5 iPhone or iPad) or Android Device(s) which law enforcement with reasonable  
6 particularity believe are in the possession or control of WAN: For the purpose of  
7 attempting to unlock the device(s) via biometric authentication in order to search its  
8 contents as authorized by this warrant, law enforcement personnel are authorized: (i) to  
9 press the fingers, including thumbs, of WAN to sensors of the device(s), or (ii) to hold up  
10 the device(s) in front of the face of WAN and activate the facial, iris, or retina recognition  
11 feature.

12 In pressing or swiping an individual's thumb or finger onto a device and in  
13 holding a device in front of an individual's face and open eyes, law enforcement may not  
14 use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,  
15 law enforcement may use no more than objectively reasonable force in light of the facts  
16 and circumstances confronting them.



**AFFIDAVIT**

STATE OF WASHINGTON ) ss  
)  
COUNTY OF KING )

I, Gary Phillips, being first duly sworn, hereby depose and state as follows:

**AFFIANT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been involved in the investigation of numerous cases involving counterintelligence.

2. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts and information in this affidavit are based upon my participation in the investigation, my review of records of others participating in the investigation, my training and experience, and information from other agents, witnesses, and agencies. Unless specifically indicated, all statements of myself or others in this affidavit are summarized in substance and in part. Also unless specifically indicated, all dates, times, or numbers are approximate.

**PURPOSE OF AFFIDAVIT**

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of the person of KUANG CHI WAN, also known as "James Wan," including any briefcase, backpack, or other bag within his possession, as described further in Attachment A, for smartphones and other communications devices to be seized and searched for records, including but not limited to a Huawei cell phone with Android ID 4497286113129079259 and serial number HWEML:BPN0218C05002044 (the "Huawei

Device”), as well as a PC laptop (the “Laptop”) (collectively, the “Devices”), as described further in Attachment B.

**PROBABLE CAUSE**

4. On January 21, 2023, KUANG CHI WAN, also known as “James Wan,” is expected to fly into Seattle-Tacoma International Airport on Korea Air KE5019 originating from Seoul, South Korea. Based on travel records, it appears that the flight originated in Taipei, Taiwan. Upon his arrival at Seattle-Tacoma International Airport, agents from the FBI intend to arrest WAN on an amended complaint signed by the Honorable Magistrate Judge Vera M. Scanlon in the Eastern District of New York on January 19, 2023, charging WAN with conspiring to acquire, transfer directly and indirectly, receive, possess, export and use one or more explosive and incendiary rockets and missiles—specifically military drones and military drone systems—in violation of Title 18, United States Code, Sections 2332g(a)(1)(A), 2332g(a)(1)(B), and 2332g(c)(1). See 22-MJ-1329 (E.D.N.Y) (VMS). The amended complaint is attached hereto as Exhibit A and incorporated by reference.

5. Based on my training and experience, I am aware that individuals who travel overseas for an extended period of time typically carry bags, luggage, and electronic devices with them. As described below, I also am aware that WAN has been using electronic devices, including the Devices, while traveling abroad. Therefore, based on my training and experience, I expect that WAN will possess electronic devices, including the Devices, with him at the time of his arrest. Because WAN traveled overseas in furtherance of his illegal scheme and has used electronic communications extensively in furtherance of his scheme, there is probable cause that his bags, luggage, electronic devices, and storage drives will contain evidence of the conspiracy.

6. Thus, the applied-for warrant would authorize the search of WAN’s person and any bag, backpack, or luggage with him and all electronic devices, storage drives, and closed and locked containers found therein, including but not limited to, the Devices.

1 The applied-for warrant also would authorize the seizure evidence, as well as forensic  
2 examination of the electronic devices for the purpose of identifying electronically stored  
3 data particularly described in Attachment B.

4 7. Since in or about 2018 to the present, WAN and various uncharged co-  
5 conspirators have been engaging in a scheme to broker sales of military drones and  
6 military drone systems manufactured by Aviation Industry Corporation of China, LTD.  
7 (“PRC Company-1” in the amended complaint) in the People’s Republic of China  
8 (“PRC”) to sanctioned countries in located in the Middle East and North Africa  
9 (“MENA”) region, including to the armed group the Libyan National Army (“Armed  
10 Group-1” in the amended complaint), in Libya (“U.N.-Sanctioned Country-1” in the  
11 amended complaint), which is a sanctioned country, through one or more shell companies  
12 based in the MENA region. WAN is a U.S. citizen who has, until recently, maintained a  
13 residence in the Eastern District of New York and resides in Canada.

14 8. As described in the amended complaint, see Exhibit A, between at least  
15 2019 and 2022, WAN has brokered numerous meetings in furtherance of his scheme to  
16 sell military drones to sanctioned countries. He also has traveled extensively in  
17 furtherance of his scheme, including to countries in the MENA region and Asia.

18 9. The investigation has revealed numerous email communications sent by  
19 WAN in connection with his scheme as well as electronic documents outlining the sale of  
20 drones to sanctioned companies. See Exhibit A ¶¶ 14-66.

21 10. In many cases, the text of the emails sent by WAN in furtherance of the  
22 scheme indicate that the emails were sent from an Android device. In other cases, the  
23 emails do not indicate they were sent from a specific device, indicating they likely were  
24 sent from a computer. For example:

25 a. On or about April 9, 2019, WAN used his Yahoo email account to  
26 ask Co-Conspirator 1 to install WeChat on his “smart phone.” He added, “Add my ID  
27 jw1088, or come to my office that I can setup for you. The communication can be more  
28

1 straight forward. You can also talk to the Chinese side directly.” The text of the email  
2 indicated that the email was “Sent from Yahoo Mail on Android.”

3           b.       On or about November 21, 2022, WAN used his Yahoo email  
4 account to forward himself a link to the “chatting history for this WeChat ‘ZXXT.’” The  
5 text of the email indicated that the email was “Sent from Yahoo Mail on Android.”  
6 ZXXT (“Front Company-1” in the amended complaint) is a PRC-based company that  
7 purports to deal in PRC-manufactured weapons, including drones and drone systems,  
8 manufactured by PRC Company-1’s subsidiaries.

9           11.     Notably, the Huawei Device is an Android device registered to WAN’s  
10 Gmail account. In turn, the contact email and recovery email addresses for WAN’s  
11 Gmail account are WAN’s business and Yahoo accounts, respectively. Further, the  
12 phone number associated with WAN’s Gmail account is the phone number known to be  
13 associated with the Huawei Device. Therefore, I assess that WAN’s Yahoo emails will  
14 be found in the Huawei Device.

15           12.     The investigation has revealed further evidence suggesting that WAN uses  
16 the electronic devices to engage in encrypted chats in furtherance of the criminal scheme.  
17 As detailed above, WAN sent emails suggesting that he was using WeChat to engage  
18 directly with counterparts in the PRC, including a group WeChat on issues related to  
19 Front Company-1. On or about October 10, 2019, WAN wrote to coconspirators  
20 (identified in the amended complaint as “Co-Conspirator 2” and “Co-Conspirator 1”) an  
21 email indicating that his WeChat ID is “jw1088,” in response to Co-Conspirator 2’s  
22 request for WAN and Co-Conspirator 1’s Viber and WeChat contact information.

23           13.     WeChat and Viber are often accessed through a mobile phone application.  
24 Application data for mobile messaging applications such as WeChat and Viber can  
25 include the content of messages sent and received, information about the user’s contacts  
26 and messaging history, and files sent and received via the mobile messaging application.

1           14. Based on my training and experience, I know that WeChat is a PRC-based  
2 communications platform that is commonly employed by individuals and people who  
3 communicate regularly with individuals based in PRC, including in some instances PRC  
4 government officials. WeChat users can send written messages, as well as voice  
5 messages and videos. Because WeChat is a PRC-based company, it does not respond to  
6 criminal process issued by the United States government, and the only manner in which  
7 the government often can obtain WeChat communications is by accessing stored WeChat  
8 communications on a smartphone or device. Based on the above-referenced  
9 conversation, I believe that WAN has a WeChat application on the Huawei Device, and  
10 that the Huawei Device likely contains information related to the conspiracy.

11           15. In addition, WAN is believed to have recently traveled with electronic  
12 devices to Morocco (“MENA Country-5” in the amended complaint) and Egypt (“MENA  
13 Country-1” in the amended complaint) to engage in the scheme to sell military drones  
14 and oil to sanctioned countries in furtherance of his illegal scheme. Based on travel  
15 records, on or about December 20, 2022, WAN flew from Montreal, Canada to Morocco  
16 on an extended business trip expected which, based on travel records, I believe will  
17 conclude in Seattle, Washington on January 21, 2023.

18           16. The purpose of WAN’s business trip and his desire to conceal his illegal  
19 activity from law enforcement officers is explained in WAN’s recent electronic  
20 communications. For example, in an email exchange with a romantic partner beginning  
21 on November 20, 2022, WAN told the romantic partner that he removed her from  
22 WeChat because he wanted to “100% concentrate[e] on my business.” The next day, on  
23 November 21, 2022, WAN wrote that he was “doing several big businesses with very top  
24 high-level leaders in the world” including a “150 billion dollar crossing 10 years in crude  
25 oil” and “more are coming.” WAN continued that he “need[ed] to remove all close  
26 friends from WeChat for now . . . to protect you [] in case any government is watching  
27 . . . trust me on what I am doing is to protect you.”

1           17. Later that day, WAN again wrote to the romantic partner that his “business  
2 is finalized and they are finalizing the payment method and banking process now, waiting  
3 for signing ceremony in December as all legal processes were completed. I am happy  
4 since it is worth 150 billion dollars. My shares are 10 M a month from February.” WAN  
5 also stated that he can “control 7% of [the] entire China oil imports market.” WAN  
6 further wrote that “the next move is Libya.” As described above, WAN previously  
7 conspired to sell military drones to Armed Group-1 in Libya which is a U.N.-sanctioned  
8 country.

9           18. WAN further wrote, “Since December, I will be traveling to China, Taiwan,  
10 Africa, middle east and south America.” Travel confirmation records in WAN’s emails  
11 showed travel from Montreal, Canada to Casablanca, Morocco, on December 20, 2022,  
12 and from Casablanca, Morocco to Cairo, Egypt on or about December 30, 2022.

13           19. Based on records from Google, WAN has accessed his Google account  
14 from a Huawei cell phone as recently as January 2, 2023, while traveling overseas. WAN  
15 also has accessed his Google account from a PC computer as recently as December 25,  
16 2022, while traveling overseas. Further, electronic records for Google and Yahoo email  
17 accounts used by WAN further reflect that on or about December 30 and 31, 2022, WAN  
18 accessed those email accounts through Internet Protocol addresses that resolve to Internet  
19 service providers located in Egypt, indicating that WAN was likely located in Egypt at  
20 the time of access.

21           20. Therefore, WAN and his bags, backpack, luggage, electronic devices  
22 (including the Devices), storage drives, and closed and locked containers, are likely to  
23 have information related to the conspiracy, including the defendant’s travel records,  
24 location data, and electronic communications about his recent business meetings, all of  
25 which are evidence of the defendant’s illegal scheme. Accordingly, there is probable  
26 cause for the search and seizure of evidence.

**CELLULAR PHONES OR WIRELESS COMMUNICATION DEVICES**

21. Cellphones or “Wireless Communication Devices” includes cellular telephones and other devices such as tablets (e.g. iPads and other similar devices) used for voice and data communication through cellular or Wi-Fi signals. These devices send signals through networks of transmitter/receivers, enabling communication with other wireless devices or traditional “land line” telephones. Many such devices can connect to the Internet and interconnect with other devices such as car entertainment systems or headsets via Wi-Fi, Bluetooth or near field communication (NFC). In addition to enabling voice communications, wireless communication devices offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books” or “contact lists;” sending, receiving, and storing short message service (SMS) and multi-media messaging service (MMS) text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; and storing dates, appointments, and other information on personal calendars.

22. Based upon my training and experience, all of these types of information may be evidence of crimes under investigation. Furthermore, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Huawei Device was used, the purpose of its use, who used it, and when. All of these types of information could constitute forensic evidence as well. Stored e-mails and text messages not only may contain communications related to crimes, but also help identify the participants in those crimes. Address books and contact lists may help identify co-conspirators. Similarly, photographs on a cellular telephone may help identify co-conspirators, either through his or her own photographs, or through photographs of friends, family, and associates. Digital photographs also often have embedded location data GPS information that identifies where the photo was taken. This



1 location information is helpful because, for example, it can show where co-conspirators  
2 meet, where they travel, and where assets might be located. Calendar data may reveal the  
3 timing and extent of criminal activity.

4 23. A cellphone used for cellular voice communication will also typically  
5 contain a “call log” or “stored list of recent, received, sent or missed calls” which records  
6 the telephone number, date, and time of calls made to and from the phone. The stored list  
7 of recent received, missed, and sent calls is important evidence. It identifies telephones  
8 recently in contact with the telephone user and may help identify co-conspirators,  
9 establish a timeline of events and/or identify who was using the phone at any particular  
10 time.

11 24. In addition, wireless communication devices will typically have an assigned  
12 number and identifying serial number such as an ESN, MIN, IMSI, or IMEI number that  
13 identifies the particular device on any network. This identifying information may also  
14 include the device’s assigned name (as assigned by the user) and network addresses such  
15 as assigned IP addresses and MAC addresses. I know based on my training and  
16 experience that such information may be important evidence of who used a device, when  
17 it was used, and for what purposes it may have been used. This information can be used  
18 to obtain toll records and other subscriber records, to identify contacts by this telephone  
19 with other telephones, or to identify other telephones used by the same subscriber or  
20 purchased as part of a package.

21 25. Many wireless communication devices including cellular telephones such  
22 as iPhones, iPads, Android phones, and other “smart phones” as well as tablet devices  
23 such as Apple iPads may also be used to browse and search the Internet. These devices  
24 may browse and search the Internet. These devices may browse and search the internet  
25 using traditional web browsers such as Apple’s Safari browser or Google’s Chrome  
26 browser as well as through third-party applications such as Facebook, Twitter and other  
27 that also provide the ability to browse and search the Internet. Based on my training and  
28

1 experience, I know that Internet browsing history may include valuable evidence  
2 regarding the identity of the user of the device. This evidence may include online user  
3 names, account numbers, e-mail accounts, and bank accounts as well as other online  
4 services. Internet browsing history may also reveal important evidence about a person's  
5 location and search history. Search history is often valuable evidence that may help  
6 reveal a suspect's intent and plans to commit a crime or efforts to hide evidence of a  
7 crime and may also help reveal the identity of the person using the device.

8         26. Cellphones and other wireless communication devices are also capable of  
9 operating a wide variety of communication application or "Apps" that allow a user to  
10 communicate with other devices via a variety of communication channels. These  
11 additional communication channels include traditional cellular networks, voice over  
12 Internet protocol, video conferencing (such as FaceTime and Skype), and wide variety of  
13 messaging applications (such as WeChat, SnapChat, What'sApp, Signal, Telegram, Viber  
14 and iMessage). I know based on my training and experience that there are hundreds of  
15 different messaging and conferencing applications available for popular cellular  
16 telephones and that the capabilities of these applications vary widely for each application.  
17 Some applications include end-to-end encryption that may prevent law enforcement from  
18 deciphering the communications without access to the device and the ability to "unlock"  
19 the device through discovery of the user's password or other authentication key.

20         27. Other communication applications transmit communications unencrypted  
21 over centralized servers maintained by the service provider and these communications  
22 may be obtained from the service provider using appropriate legal process. Other  
23 applications facilitate multiple forms of communication including text, voice, and video  
24 conferencing. Information from these communication apps may constitute evidence of  
25 crimes under investigation to the extent they may reveal communications related to the  
26 crime or evidence of who the user of the device was communicating with and when those  
27

1 | communications occurred. Information from these communication apps may also reveal  
2 | alias names used by the device owner that may also lead to the other evidence.

3 |       28. I know based on my training and experience that obtaining a list of all the  
4 | applications present on a cellphones may provide valuable leads in an investigation. By  
5 | determining what applications are present on a device, an investigator may conduct  
6 | follow-up investigation including obtaining subscriber records and logs to determine  
7 | whether the device owner or operator has used each particular messaging application.  
8 | This information may be used to support additional search warrants or other legal process  
9 | to capture those communications and discover valuable evidence.

10 |       29. Cellphones and other wireless communication devices may also contain  
11 | geolocation information where the device was a particular times. Many of these devices  
12 | track and store GPS and cell-site location data to provide enhanced location-based  
13 | services, serve location-targeted advertising, search results, and other content. Numerous  
14 | applications available for wireless communication devices collect and store location data.  
15 | For example, when location services are enabled on a handheld mobile device, many  
16 | photo applications will embed location data with each photograph taken and stored on the  
17 | device. Mapping applications such as Google Maps may store location data including  
18 | lists of locations the user has entered into the application. Location information may  
19 | constitute evidence of the crimes under investigation because that information may reveal  
20 | whether a suspect was at or near the scene of a crime at any given moment and may also  
21 | reveal evidence related to the identity of the user of the device.

22 |       30. Based on my training and experience, and research, I know that cellular  
23 | phones like the Huawei have capabilities that allow them to function as a wireless  
24 | telephones, digital camera, portable media player, GPS navigation device, and "PDA." In  
25 | my training and experience, examining data stored on devices of this type can uncover,  
26 | among other things, evidence that reveals or suggests who possessed or used the device.  
27 |  
28 |

1 In my training and experience, smart phones can act as mini-computers in that they have  
2 many of the functionalities of traditional computers.

3 31. Searching a cellular phone or wireless communication device is frequently  
4 different than conducting a search of a traditional computer. Agents and forensic  
5 examiners will attempt to extract the contents of the cellular phone or wireless  
6 communication device using a variety of techniques designed to accurately capture the  
7 data in a forensically sound manner in order to make data available to search of items  
8 authorized by the search warrant. This may involve extracting a bit-for-bit copy of the  
9 contents of the device or, if such an extraction is not feasible for any particular device,  
10 the search may involve other methods of extracting data from the device, such as copying  
11 the device's active user files (known as a logical acquisition) or copying the device's  
12 entire file system (known as a file system acquisition). If none of these methods are  
13 supported by the combination of tools available to the examiner and the device to be  
14 searched, the agents and examiners may conduct a manual search of the device by  
15 scrolling through the contents of the device and photographing the results. Based on the  
16 foregoing and consistent with Rule 41(e)(2)(B), the warrant I am applying for would  
17 permit seizing, imaging, or otherwise copying the Huawei Device and would authorize a  
18 later review of the media or information consistent with the warrant. The later review  
19 may require techniques, including but not limited to computer-assisted scans of the entire  
20 medium, that might expose many parts of a hard drive to human inspection in order to  
21 determine whether it is evidence described by the warrant.

22 **COMPUTER, ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

23 32. Based on my knowledge, training, and experience, I know that electronic  
24 devices can store information for long periods of time. Similarly, things that have been  
25 viewed via the Internet are typically stored for some period of time on the device. This  
26 information can sometimes be recovered with forensics tools.

1        33. There is probable cause to believe that things that were once stored on  
2 Devices such as the Laptop may still be stored there, for at least the following reasons:

3        34. Based on my knowledge, training, and experience, I know that computer  
4 files or remnants of such files can be recovered months or even years after they have been  
5 downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files  
6 downloaded to a storage medium can be stored for years at little or no cost. Even when  
7 files have been deleted, they can be recovered months or years later using forensic tools.  
8 This is so because when a person “deletes” a file on a computer, the data contained in the  
9 file does not actually disappear; rather, that data remains on the storage medium until it is  
10 overwritten by new data.

11        35. Therefore, deleted files, or remnants of deleted files, may reside in free  
12 space or slack space—that is, in space on the storage medium that is not currently being  
13 used by an active file—for long periods of time before they are overwritten. In addition,  
14 a computer’s operating system may also keep a record of deleted data in a “swap” or  
15 “recovery” file.

16        36. Wholly apart from user-generated files, computer storage media—in  
17 particular, computers’ internal hard drives—contain electronic evidence of how a  
18 computer has been used, what it has been used for, and who has used it. To give a few  
19 examples, this forensic evidence can take the form of operating system configurations,  
20 artifacts from operating system or application operation, file system data structures, and  
21 virtual memory “swap” or paging files. Computer users typically do not erase or delete  
22 this evidence, because special software is typically required for that task. However, it is  
23 technically possible to delete this information.

24        37. Similarly, files that have been viewed via the Internet are sometimes  
25 automatically downloaded into a temporary Internet directory or “cache.”

26        38. *Forensic evidence.* As further described in Attachment B, this application  
27 seeks permission to locate not only electronically stored information that might serve as  
28

1 direct evidence of the crimes described on the warrant, but also forensic evidence that  
2 establishes how the Devices were used, the purpose of its use, who used it, and when.  
3 There is probable cause to believe that this forensic electronic evidence might be on the  
4 Devices because:

5           a.       Data on the storage medium can provide evidence of a file that was  
6 once on the storage medium but has since been deleted or edited, or of a deleted portion  
7 of a file (such as a paragraph that has been deleted from a word processing file). Virtual  
8 memory paging systems can leave traces of information on the storage medium that show  
9 what tasks and processes were recently active. Web browsers, e-mail programs, and chat  
10 programs store configuration information on the storage medium that can reveal  
11 information such as online nicknames and passwords. Operating systems can record  
12 additional information, such as the attachment of peripherals, the attachment of USB  
13 flash storage devices or other external storage media, and the times the computer was in  
14 use. Computer file systems can record information about the dates files were created and  
15 the sequence in which they were created.

16           b.       As explained herein, information stored within a computer and other  
17 electronic storage media may provide crucial evidence of the “who, what, why, when,  
18 where, and how” of the criminal conduct under investigation, thus enabling the United  
19 States to establish and prove each element or alternatively, to exclude the innocent from  
20 further suspicion. In my training and experience, information stored within a computer  
21 or storage media (e.g., registry information, communications, images and movies,  
22 transactional information, records of session times and durations, internet history, and  
23 anti-virus, spyware, and malware detection programs) can indicate who has used or  
24 controlled the computer or storage media. This “user attribution” evidence is analogous  
25 to the search for “indicia of occupancy” while executing a search warrant at a residence.  
26 The existence or absence of anti-virus, spyware, and malware detection programs may  
27 indicate whether the computer was remotely accessed, thus inculcating or exculpating the  
28

1 computer owner and/or others with direct physical access to the computer. Further,  
2 computer and storage media activity can indicate how and when the computer or storage  
3 media was accessed or used. For example, as described herein, computers typically  
4 contain information that log: computer user account session times and durations,  
5 computer activity associated with user accounts, electronic storage media that connected  
6 with the computer, and the IP addresses through which the computer accessed networks  
7 and the internet. Such information allows investigators to understand the chronological  
8 context of computer or electronic storage media access, use, and events relating to the  
9 crime under investigation.<sup>1</sup> Additionally, some information stored within a computer or  
10 electronic storage media may provide crucial evidence relating to the physical location of  
11 other evidence and the suspect. For example, images stored on a computer may both  
12 show a particular location and have geolocation information incorporated into its file  
13 data. Such file data typically also contains information indicating when the file or image  
14 was created. The existence of such image files, along with external device connection  
15 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
16 camera or cellular phone with an incorporated camera). The geographic and timeline  
17 information described herein may either inculcate or exculpate the computer user. Last,  
18 information stored within a computer may provide relevant insight into the computer  
19 user's state of mind as it relates to the offense under investigation. For example,  
20 information within the computer may indicate the owner's motive and intent to commit a  
21 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt  
22 (e.g., running a "wiping" program to destroy evidence on the computer or password  
23 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

---

25 <sup>1</sup> For example, if the examination of a computer shows that: a) at 11:00am, someone  
26 using the computer used an internet browser to log into a bank account in the name of John Doe;  
27 b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am  
28 the internet browser was used to log into a social media account in the name of John Doe, an  
investigator may reasonably draw an inference that John Doe downloaded child pornography.



1 c. A person with appropriate familiarity with how an electronic device  
2 works may, after examining this forensic evidence in its proper context, be able to draw  
3 conclusions about how electronic devices were used, the purpose of their use, who used  
4 them, and when.

5 d. The process of identifying the exact electronically stored  
6 information on a storage medium that are necessary to draw an accurate conclusion is a  
7 dynamic process. Electronic evidence is not always data that can be merely reviewed by  
8 a review team and passed along to investigators. Whether data stored on a computer is  
9 evidence may depend on other information stored on the computer and the application of  
10 knowledge about how a computer behaves. Therefore, contextual information necessary  
11 to understand other evidence also falls within the scope of the warrant.

12 e. Further, in finding evidence of how a device was used, the purpose  
13 of its use, who used it, and when, sometimes it is necessary to establish that a particular  
14 thing is not present on a storage medium.

15 39. *Manner of execution.* Because this warrant seeks only permission to  
16 examine devices seized from WAN upon his arrival in the United States, the execution of  
17 this warrant does not involve the physical intrusion onto a premises. Consequently, I  
18 submit there is reasonable cause for the Court to authorize execution of the warrant at any  
19 time in the day or night.

20  
21 **PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION**

22 40. In the Course of this investigation, the government has obtained ESI from  
23 other sources including search warrants to Google, Apple, Yahoo, Zoom, and subpoenas  
24 to Google, Apple, Yahoo, T-Mobile, AT&T, LinkedIn, and PayPal, among other  
25 providers.

## SEARCH TECHNIQUES

41. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the electronic devices, and will specifically authorize a review of the media or information consistent with the warrant.

42. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the electronic devices pursuant to this warrant as follows:

### **a. Securing the Data**

43. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the electronic devices.

44. Law enforcement will only create an image of data physically present on or within the electronic devices. Creating an image of the electronic devices will not result in access to any data physically located elsewhere. However, the electronic devices that have previously connected to devices at other locations may contain data from those other locations.

### **b. Searching the Forensic Images**

45. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and

1 protocols as may reasonably be expected to find, identify, segregate and/or duplicate the  
2 items authorized to be seized pursuant to Attachment B to this affidavit.

3 **c. Biometrics**

4 46. The warrant I am applying for would permit law enforcement to obtain  
5 from certain individuals the display of physical biometric characteristics (such as  
6 fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to  
7 search and seizure pursuant to this warrant. I seek this authority based on the following:

8 a. I know from my training and experience, as well as from  
9 information found in publicly available materials published by device manufacturers, that  
10 many electronic devices, particularly newer mobile devices and laptops, offer their users  
11 the ability to unlock the device through biometric features in lieu of a numeric or  
12 alphanumeric passcode or password. These biometric features include fingerprint  
13 scanners and facial recognition features. Some devices offer a combination of these  
14 biometric features, and the user of such devices can select which features they would like  
15 to utilize.

16 b. If a device is equipped with a fingerprint scanner, a user may enable  
17 the ability to unlock the device through his or her fingerprints. For example, Apple offers  
18 a feature called "Touch ID," which allows a user to register up to five fingerprints that  
19 can unlock a device. Once a fingerprint is registered, a user can unlock the device by  
20 pressing the relevant finger to the device's Touch ID sensor, which is found in the round  
21 button (often referred to as the "home" button) located at the bottom center of the front of  
22 the device. The fingerprint sensors found on devices produced by other manufacturers  
23 have different names but operate similarly to Touch ID.

24 c. If a device is equipped with a facial recognition feature, a user may  
25 enable the ability to unlock the device through his or her face, iris, or retina. For example,  
26 Apple offers a facial recognition feature called "Face ID." During the Face ID  
27 registration process, the user holds the device in front of his or her face. The device's

1 camera then analyzes and records data based on the user's facial characteristics. The  
2 device can then be unlocked if the camera detects a face with characteristics that match  
3 those of the registered face. Facial recognition features found on devices produced by  
4 other manufacturers have different names but operate similarly to Face ID.

5 d. While not as prolific on digital devices as fingerprint and facial-  
6 recognition features, both iris and retina scanning features exist for securing devices/data.  
7 The human iris, like a fingerprint, contains complex patterns that are unique and stable.  
8 Iris recognition technology uses mathematical pattern-recognition techniques to map the  
9 iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye  
10 to map the unique variations of a person's retinal blood vessels. A user can register one  
11 or both eyes to be used to unlock a device with these features. To activate the feature, the  
12 user holds the device in front of his or her face while the device directs an infrared light  
13 toward the user's face and activates an infrared sensitive camera to record data from the  
14 person's eyes. The device is then unlocked if the camera detects the registered eye.

15 e. In my training and experience, users of electronic devices often  
16 enable the aforementioned biometric features because they are considered to be a more  
17 convenient way to unlock a device than by entering a numeric or alphanumeric passcode  
18 or password. Moreover, in some instances, biometric features are considered to be a more  
19 secure way to protect a device's contents. This is particularly true when the users of a  
20 device are engaged in criminal activities and thus have a heightened concern about  
21 securing the contents of a device.

22 f. As discussed in this affidavit, based on my training and experience I  
23 believe that one or more digital devices will be found during the search. The passcode or  
24 password that would unlock the device(s) subject to search under this warrant is not  
25 known to law enforcement. Thus, law enforcement personnel may not otherwise be able  
26 to access the data contained within the device(s), making the use of biometric features  
27 necessary to the execution of the search authorized by this warrant.

1           g. I also know from my training and experience, as well as from  
2 information found in publicly available materials including those published by device  
3 manufacturers, that biometric features will not unlock a device in some circumstances  
4 even if such features are enabled. This can occur when a device has been restarted,  
5 inactive, or has not been unlocked for a certain period of time. For example, Apple  
6 devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed  
7 since the device was last unlocked or (2) when the device has not been unlocked using a  
8 fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156  
9 hours. Biometric features from other brands carry similar restrictions. Thus, in the event  
10 law enforcement personnel encounter a locked device equipped with biometric features,  
11 the opportunity to unlock the device through a biometric feature may exist for only a  
12 short time.

13           h. In my training and experience, the person who is in possession of a  
14 device or has the device among his or her belongings at the time the device is found is  
15 likely a user of the device. However, in my training and experience, that person may not  
16 be the only user of the device, and may not be the only individual whose physical  
17 characteristics are among those that will unlock the device via biometric features.  
18 Furthermore, while physical proximity is an important factor in determining who is the  
19 user of a device, it is only one among many other factors that may exist.

20           i. Due to the foregoing, I request that if law enforcement personnel  
21 encounter a device that is subject to search and seizure pursuant to this warrant and may  
22 be unlocked using one of the aforementioned biometric features, and if law enforcement  
23 reasonably believes KUANG CHI WAN, also known as “James Wan,” is a user of the  
24 device, then – for the purpose of attempting to unlock the device in order to search the  
25 contents as authorized by this warrant – law enforcement personnel shall be authorized  
26 to:(1) press or swipe the fingers (including thumbs) of WAN to the fingerprint scanner of  
27  
28

1 the device; and/or (2) hold the device in front of the face and open eyes of WAN and  
2 activate the facial, iris, or retina recognition feature.

3 47. In pressing or swiping an individual's thumb or finger onto a device and in  
4 holding a device in front of an individual's face and open eyes, law enforcement may not  
5 use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,  
6 law enforcement may use no more than objectively reasonable force in light of the facts  
7 and circumstances confronting them.

8 **REQUEST FOR SEALING**

9 48. It is respectfully requested that this Court issue an order sealing, until  
10 further order of the Court, all papers submitted in support of this application, including  
11 the application and search warrant. I believe that sealing these documents is necessary  
12 because the warrant is relevant to an ongoing investigation, and not all of the targets of  
13 this investigation will be searched at this time. Furthermore, the targets are not aware of  
14 the investigation, or at least of the full scope of the investigation. Based upon my training  
15 and experience, I have learned that criminals actively search for criminal affidavits and  
16 search warrants via the internet and disseminate them to other criminals as they deem  
17 appropriate. Premature disclosure of the contents of this affidavit and related documents  
18 may have a significant and negative impact on the continuing investigation and may  
19 severely jeopardize its effectiveness. It could cause some targets to flee or avoid returning  
20 to the United States, to destroy or tamper with evidence, to intimate other potential  
21 witnesses, or otherwise seriously jeopardize the investigation.  
22  
23  
24  
25  
26  
27  
28

**CONCLUSION**

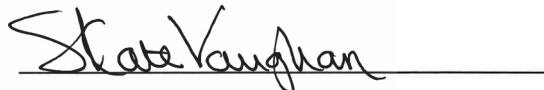
49. Based upon the information set forth above, I respectfully submit that there is probable cause to search the person described in Attachment A for smartphones and other communications devices to be seized and searched for records, as described further in Attachment B.



GARY PHILLIPS, Affiant

Special Agent, FBI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on January 20, 2023.



HONORABLE S. KATE VAUGHAN

United States Magistrate Judge



## **EXHIBIT A (EDNY Complaint)**

**HSD AND SEALED**

DMP/CRH:AAS/ICR/SKW  
F. #2020R00969

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

KUANG CHI WAN,  
also known as "James Wan,"

Defendant.

----- X

EASTERN DISTRICT OF NEW YORK, SS:

GARY PHILLIPS, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

In or about and between 2018 and the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant KUANG CHI WAN, also known as "James Wan," together with others, did knowingly and intentionally conspire to acquire, transfer directly and indirectly, receive, possess, export and use one or more explosive and incendiary rockets and missiles that are guided by systems designed to enable the rockets and missiles to direct and guide the rockets and missiles to an aircraft and certain devices designed or intended to launch or guide such rockets or missiles, to wit: various air-to-air and surface-to-air rockets or missiles, including certain man-portable air defense systems

**TO BE FILED UNDER SEAL**

AMENDED COMPLAINT  
AND AFFIDAVIT IN  
SUPPORT OF APPLICATION  
FOR ARREST WARRANT

(18 U.S.C. §§ 2332g(a)(1)(A),  
2332g(a)(1)(B), 2332g(c)(1))

No. 22-MJ-1329

**HSD AND SEALED**

2

(“MANPADS”), and various military drones and military drone systems, including the Wing Loong II drone.

(Title 18, United States Code, Sections 2332g(a)(1)(A), 2332g(a)(1)(B), 2332g(c)(1)).

The source of your deponent’s information and the grounds for his belief are as follows:<sup>1</sup>

1. I am a Special Agent with the FBI and have been involved in the investigation of numerous cases involving counterintelligence. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file; and from reports of other law enforcement officers involved in the investigation.

The Defendant and Co-Conspirators

2. The defendant KUANG CHI WAN, also known as “James Wan,” is a U.S. citizen who, until in or about June 2022, maintained a residence in Queens County, New York. WAN’s principal residence is in Montreal, Canada. Until this past year, WAN was employed as Deputy Director of Administration and Services for the International Civil Aviation Organization (“ICAO”), which is a United Nations (“U.N.”) agency based in Montreal, Canada that develops policies and standards for the global civil aviation system. Notably, ICAO’s remit has expanded into the area of unmanned aircraft systems (“UAS,” i.e., drones), whereby ICAO has developed a model regulatory framework as well as additional guidance and training for U.N. member states.

---

<sup>1</sup> Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.



**HSD AND SEALED**

3

3. PRC Company-1 is a People's Republic of China ("PRC" or "China") state-owned aerospace and defense conglomerate based in Beijing that directly and indirectly owns and controls numerous publicly acknowledged subsidiary entities through which, and among other things, it manufactures and distributes civilian and military aircraft. In November 2020, the President issued Executive Order ("E.O.") 13959, which prohibited U.S. investors from purchasing or investing in securities of companies identified by the U.S. Department of Defense as a "Communist Chinese military company." See E.O. 13959, 85 Fed. Reg. 73185 (Nov. 17, 2020). PRC Company-1 was designated as such a company in the Annex to the Executive Order. Id. In June 2021, the President issued Executive Order 14032, which superseded and expanded the scope of Executive Order 13959 and shifted the responsibility for making designations under the sanctions program to the U.S. Department of the Treasury. See E.O. 14032, 86 Fed. Reg. 30145 (June 7, 2021). PRC Company-1 remains sanctioned under Executive Order 14032, now overseen by Treasury's Office of Foreign Assets Control, as a "Non-SDN Chinese Military-Industrial Complex Company." In many of the documents described below, PRC Company-1 and some of its direct and indirectly held subsidiaries are referred to generically by an acronym common to many of the entities within the PRC Company-1 group of companies. Accordingly, in this affidavit, and unless otherwise indicated, I refer to PRC Company-1 and its publicly acknowledged subsidiaries as "PRC Company-1."

4. Front Company-1 and Front Company-2 are PRC-based entities ostensibly separate from PRC Company-1 that purport to deal in PRC-manufactured weapons, including in the case of Front Company-1, drones and drone systems manufactured by PRC Company-1's subsidiaries. As detailed below, while Front Company-1 and Front Company-2 are not publicly acknowledged as controlled by PRC Company-1, the investigation has revealed evidence that

**HSD AND SEALED**

4

Front Company-1 is being used as a proxy for PRC Company-1 and its subsidiaries, allowing PRC Company-1 to transact with prospective clients and customers, including customers in countries subject to sanctions measures, without creating a record of a transaction directly with PRC Company-1. In addition, and as detailed below, some members of the conspiracy hold executive positions at both Front Company-1 and Front Company-2, and have offered, on behalf of Front Company-2, to sell unspecified PRC-manufactured weapons to end-users in a country subject to U.N. sanctions measures.

5. Co-Conspirator 1 is a national of a country that, at all times relevant to this Amended Complaint, was subject to sanctions measures relating to, among other things, defense articles and services, mandated by the United Nations Security Council (hereinafter “U.N.-Sanctioned Country-1”). Co-Conspirator 1 was previously employed by ICAO as an “Aviation Security and Facilitation Policy Section Consultant.”

6. Co-Conspirator 2 is a Canadian citizen and was previously employed by ICAO as the Supervisor, Property Control & Logistics and Commissariat Manager. Co-Conspirator 2 resides in Montreal, Canada.

7. Co-Conspirator 3 is a Senior Vice President of Front Company-1. According to documents obtained during the investigation, Co-Conspirator 3 has also acted as a representative for Front Company-2.

8. Co-Conspirator 4 is the Chairman of Front Company-1 and has also acted as a representative for Front Company-2.

9. Co-Conspirator 5 is a citizen of a country located in the Middle East and North Africa (“MENA”) region (“MENA Country-1”) and the principal of two shell companies registered in a different country also located in the MENA region (“MENA Country-2”),



**HSD AND SEALED**

5

including what is referred to herein as MENA Entity-1 and MENA Entity-2. Co-Conspirator 5 resides in MENA Country-1.

10. Co-Conspirator 6 is a PRC national who is the principal of an entity based in the United Kingdom (“U.K.”), U.K. Company-1.

Overview of the Criminal Scheme

11. Since in or about 2018 to the present, the defendant and various co-conspirators are engaging in a scheme to broker sales of military drones and military drone systems manufactured by PRC Company-1 in the PRC to end users in the MENA region, including to an armed group based in U.N.-Sanctioned Country-1 (“Armed Group-1”), through one or more shell companies based in the MENA region. As noted above, WAN is a U.S. citizen who has, until recently, maintained a residence in the Eastern District of New York and who is therefore within the jurisdiction of the United States under 18 U.S.C. § 2332g(b)(2). In addition, the scheme described herein occurred in and affecting interstate and foreign commerce. See 18 U.S.C. § 2332g(b)(1).

12. A document that metadata reveals was last modified by WAN found in WAN’s files dated July 20, 2020, titled “Initialization of the relationship between [U.N.-Sanctioned Country-1] and China-James (final)” narrates certain key events of the criminal scheme through the summer of 2020. According to the document, in or about late 2019, WAN and Co-Conspirator 1 first conceived of working with PRC Company-1 and Front Company-1 to assist Armed Group-1 to “secure the necessary equipment” for the purpose of “‘using war to end the war quick.’” Based on my training and experience, I assess that the “necessary equipment” described in this document refers to what appear to be combat capable defense articles. Co-Conspirator 4 (whom WAN identified as a special advisor to PRC President Xi Jinping) and Co-

**HSD AND SEALED**

6

Conspirator 3 would negotiate directly with Armed Group-1 in their capacities as representatives of Front Company-2. As described in the document, Front Company-2 was a special entity specifically authorized by the PRC government to engage in international business outside the purview of the PRC's Ministry of Foreign Affairs, so that the PRC's Ministry of Foreign Affairs would not appear to play a role in negotiations with Armed Group-1. As WAN explained in the document:

At the end of 2019, [Co-Conspirator 1] approached me for seeking collaborations in projects associated with the development of [U.N.-Sanctioned Country-1]. I immediately contacted [Co-Conspirator 4], a special adviser to the Presiden[t] of China, President Xi, for his consideration. After a series of profound analysis in China, [Co-Conspirator 4] submitted a constructive report to the President for his instruction.

....

[Co-Conspirator 4]'s advice to the President was that China, as a responsible country keeping global peace and focusing on people's well being, should place herself in an active position to assist [U.N.-Sanctioned Country-1] to end the war and become a unified state that is the best and top interest of [U.N.-Sanctioned Country-1] people and the global society. With the endorsement from the President, the instruction from him was to support [U.N.-Sanctioned Country-1] to end the war for the sake of [U.N.-Sanctioned Country-1] people.

....

Due to the lack of understanding of the current [U.N.-Sanctioned Country-1] situation, the President asked [Co-Conspirator 4] and [Co-Conspirator 3] to visit [U.N.-Sanctioned Country-1] informally (without the involvement of the Foreign Affairs to ensure its independence) and to meet the leaders of [U.N.-Sanctioned Country-1] in February 2020. The objectives were to assess the facts that happen in [U.N.-Sanctioned Country-1] and make a recommendation in terms of tangible actions reporting back to him.

....

The President gave his final instruction to move forward in actions backing the [leader of Armed Group-1]. At the moment, both the ministry of Foreign Affairs and [PRC Company-1] with [Front Company-1] are instructed to realize his direction in helping [U.N.-Sanctioned Country-1] to secure necessary equipment, and China also committed herself to establishing a full partnership in



**HSD AND SEALED**

7

national corporations, including investments in the development of the country, with [U.N.-Sanctioned Country-1] after this initiating project being concluded.

....

Based on President Xi's instruction in January 2020, considering both the urgent situation in [U.N.-Sanctioned Country-1] and the complication of the Foreign Affairs climate could unnecessarily disclose such strategic movement, which for sure will increase the difficulties in supporting [U.N.-Sanctioned Country-1] effectively. Based on that consideration, [Front Company-2] was appointed to be the focal point company from China's end as the first step of building up the connection for both parties.

The main reason for such a decision was grounded on that [Front Company-2] is one of the specially authorized companies in China to conduct all international business activities independently, which means [Front Company-2] is licensed and approved by the Foreign Affairs ministry and the Commercial ministry of China as a legally autonomous entity. Because of [Front Company-2's] unique position, China's Foreign Affairs system was not involved in the realization of the project during this period of the first phase.<sup>2</sup>

Notably, an attachment to an email from Co-Conspirator 4 to WAN described Co-Conspirator 4 as a "consultant to the Chinese government."

13. WAN's document also detailed how Armed Group-1 was initially distrustful of Front Company-2, which was an entity unknown to Armed Group-1. Accordingly, the PRC government determined to have PRC Company-1/Front Company-1 negotiate with Armed Group-1 in full coordination with the PRC's Ministry of Foreign Affairs. As part of this strategy, the PRC government planned to invite U.N.-Sanctioned Country-1 leadership to the PRC to discuss the sale of PRC Company-1/Front Company-1 military drones and drone systems. In part to induce what WAN described as the government of U.N.-Sanctioned Country-1 to purchase PRC Company-1/Front Company-1 products and services, the PRC government would authorize PRC Company-1 and Front Company-1 to donate medical supplies

---

<sup>2</sup> All citations to electronic communications include original spelling, punctuation, and grammar.

**HSD AND SEALED**

8

and equipment, including PRC-manufactured COVID-19 vaccines. In the same document, WAN explained the distrust from potential customers in U.N.-Sanctioned Country-1 of Front Company-2 as follows:

However, attribute to that, that particular arrangement resulted in a massive misunderstanding from [U.N.-Sanctioned Country-1]. Through the intelligence verification process with the traditional channel, the contacts [U.N.-Sanctioned Country-1] could reach, due to lack of involvement from this sensitive project, they could not confirm the situation.

Owing to such misunderstanding, the whole project is turning into suspicion from [U.N.-Sanctioned Country-1] that, in return, hurts China and the President from their good intention and effort to assist [U.N.-Sanctioned Country-1] to become a unified country.

To address [U.N.-Sanctioned Country-1]'s concerns, China was willing to start phase two of the project, which involves the official government channel, even taking with the risks of exploring such strategic movement with [U.N.-Sanctioned Country-1]. Accordingly, after the regular report and the approval of the President, [Co-Conspirator 4] started engaging [PRC Company-1] (a ministry-level national owned, and also a global fortune 500 company) and the Foreign Affairs ministry for collaboratively implementing this project. [PRC Company-1] and [Front Company-1] are supported and authorized by the Foreign Affairs ministry as focal point companies of China's end initiating the donation against the Coronavirus.

At this moment, involved senior officials including director-general, deputy director-general, and directors in charge of Chinese Foreign Affairs matters in the West Asia and North Africa region in the Foreign Affairs ministry have been officially informed and asked to provide active supports to finish this project immediately. Because of that, the Foreign Affairs and [PRC Company-1] established a dedicated inter-ministerial working team to handle this case that seldomly happens in the Chinese government's history. After that moment, the global climate has changed dramatically. The Chinese government still commits herself to support the [U.N.-Sanctioned Country-1] people and her representative to end the civil war.

At this moment, all proposed and associated equipment (including contract proposal and approval of exporting such equipment) and senior Chinese officials are ready to meet [U.N.-Sanctioned Country-1]'s senior officials to conclude this first project.



**HSD AND SEALED**

9

....  
Considering its priority, the Chinese government would like to invite senior [U.N.-Sanctioned Country-1] officials to visit China with a special entry arrangement to conclude this project. Both the Foreign Affairs ministry and [PRC Company-1] will send their official invitation letters upon received the scanned copies of invitees' passport.

Notably, WAN and Co-Conspirators 1 and 2 did not engage in the brokering of military drone systems as part of their official duties at ICAO. Indeed, WAN and Co-Conspirators 1 and 2 regularly communicated through personal email accounts and used personal videotelephony software programs to discuss their brokering activities.

14. Correspondence obtained during the investigation reflects that the ongoing brokering scheme pertained to military drones and drone systems manufactured by PRC Company-1. In an email WAN received on or about December 27, 2020, from a PRC Company-1 employee, PRC Company-1 attached brochures for Front Company-1 and another PRC Company-1 subsidiary ("PRC Subsidiary-1").<sup>3</sup> The Front Company-1 brochure stated that Front Company-1 was involved in selling weapons systems, including drones with strike capabilities. The brochure described Front Company-1's products as follows:

[Front Company-1] provides a flexible configuration of three types of air motorized platforms (AMP) in the above typical applications. That is

1. Large-scale AMP (strategic-level application)
  - ☐ Mission payload: 500kg
  - ☐ Modular double-engine (strong robustness), multi-role medium altitudelong endurance
  - ☐ Autonomous flight as planned in the mission
  - ☐ Reconnaissance and strike for long range and high altitude (8.5km of Max. ceiling altitude).

---

<sup>3</sup> PRC Subsidiary-1 is described in the brochure as a "a wholly-owned subsidiary of [PRC Company-1]."

**HSD AND SEALED**

10

15. Later correspondence clarified that the PRC Company-1 products at issue included the Wing Loong II drone, among other military drone systems. An open-source picture depicting the Wing Loong II drone is below.



16. Another PRC Company-1/Front Company-1 product that is the object of the brokering scheme is the New Generation Emergency Communications System (“NGECS”), which is sold as a package with other PRC Company-1/Front Company-1 products. Documents from WAN’s emails reflect that the NGECS package consists of, among other components, three types of drones, at least two of which are weapons capable, command and control infrastructure to operate PRC Company-1/Front Company-1 drones, and equipment for anti-drone countermeasures. Notably, drones are classified as aircraft under 18 U.S.C. § 2332g. On or about March 8, 2021, WAN sent an email to Co-Conspirator 1 attaching a document about NGECS that WAN indicated would answer any technical questions. The document reflected the types of drones included in NGECS, including an image of a drone with weapons affixed to the wings—further corroboration that the NGECS package has military applications.



**HSD AND SEALED**

11

17. An unsigned letter dated September 23, 2021, sent to WAN by Co-Conspirator 4 addressed to the “Military Attaché of [MENA Country-1] Embassy in China” further clarified the military applications of the NGECS package. The letter described a project involving MENA Country-1’s procurement of “cutting-edge drones” from China. According to the letter, the drones included in the NGECS include “an intelligence-based communication network and contain[] the built-in world-leading technologies of jamming functionalities,” and will assist with “strategic point security or any expanded system covering the whole territory of [MENA Country-1].” The “basic configuration specifies,” among other components, “[u]nmanned aerial vehicle upon customer’s needs.”

WAN and Co-Conspirator 1 Initiate the Scheme to Sell Weapons

18. Though WAN wrote in his July 2020 narrative that he and Co-Conspirator 1 first discussed a joint venture involving selling military drones to Armed Group-1 in late 2019, WAN and Co-Conspirators 1 and 2 attempted to coordinate a meeting with Co-Conspirator 3 in New York City in late 2018 and early 2019. On February 10, 2019, WAN wrote Co-Conspirators 1 and 2, indicating that he had “[j]ust received a call from China. They asked if we could meet in NY city.” After Co-Conspirator 1 responded that he would need to apply for a visa, WAN wrote, “I need a confirmation ASAP if you can go to New York this weekend since they [Co-Conspirator 3 and others] have to buy the tickets immediately.” Co-Conspirator 1 indicated that the visa processing time would preclude his attendance and asked for other times that would work for rescheduling.

19. Subsequently, WAN and Co-Conspirators 1 and 2 met with Armed Group-1 representatives in a third country located in the MENA region (“MENA Country-3”) as early as late March and early April 2019.



**HSD AND SEALED**

12

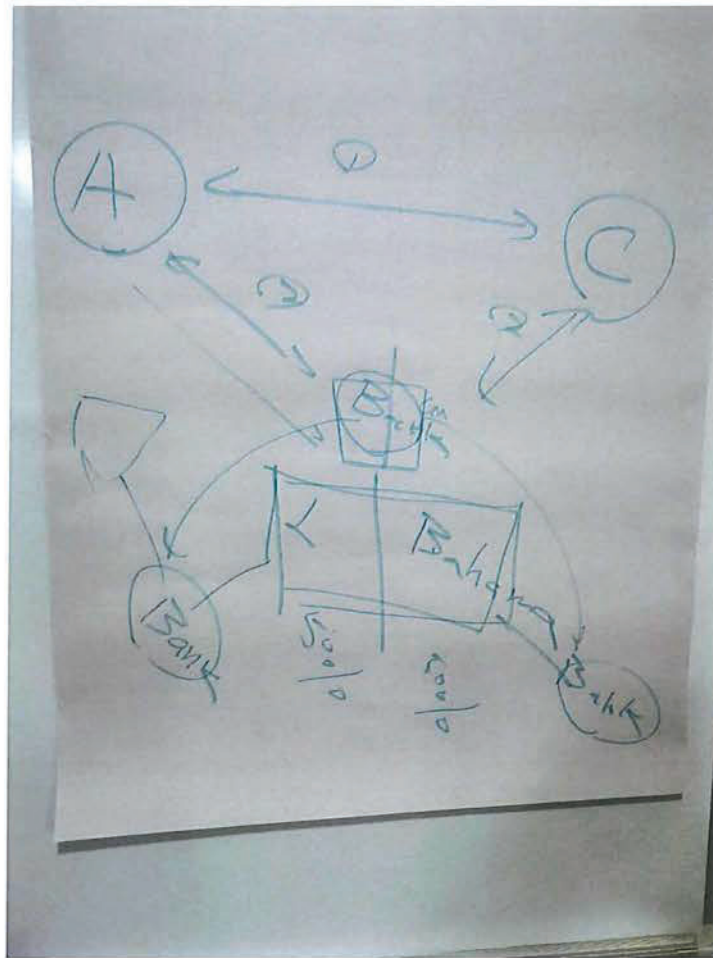


The picture above depicts WAN (on the far left), a suspected Armed Group-1 member whose face has been obscured, Co-Conspirator 1 whose face has been obscured, another suspected Armed Group-1 member whose face has been obscured, Co-Conspirator 2 whose face has been obscured, and Co-Conspirator 6 (on the far right) whose face has been obscured. The metadata of the photograph reflects a creation date of April 1, 2019, and geolocation data associated with a hotel in the capital city of MENA Country-3.

20. Related photographs suggest that, during these meetings in the capital city of MENA Country-3, WAN and Co-Conspirators 1 and 2 discussed using various shell entities in furtherance of the transactions. For example, the following photo, whose metadata reflects a creation date of March 30, 2019—two days before the photograph described above—and is geolocated to the same hotel, depicts a diagram showing flows of money from two entities through three banks, including a bank in the Bahamas.

**HSD AND SEALED**

13



21. The investigation has not uncovered additional documents suggesting that a transaction with Front Company-2 was, in fact, consummated following the 2019 meeting in MENA Country-3. However, as noted in WAN's narrative document, Armed Group-1 was not initially receptive to overtures made through Front Company-2.

Phase Two of the Scheme to Sell Weapons

22. According to WAN's narrative, the second phase of the scheme began after the PRC government determined to have PRC Company-1/Front Company-1 interface directly with the U.N.-Sanctioned Country-1 government with assistance from the PRC's



**HSD AND SEALED**

14

Ministry of Foreign Affairs. Accordingly, Co-Conspirators 3 and 4 contacted Armed Group-1 representatives to arrange an in-person meeting in the PRC in early 2020.

23. On or about December 30, 2019, Co-Conspirator 4 wrote to the leader of Armed Group-1 on Front Company-1's letterhead, inviting the leader and his representatives to visit the PRC in January 2020 "for a high level meeting discussing about future cooperation between us." Co-Conspirator 4 signed the letter as "Chairman" of Front Company-1, and the letter referenced Co-Conspirator 3 as Front Company-1's "Coordinator." Co-Conspirator 4 wrote that Co-Conspirator 1 and WAN were the "authorized coordinators of the events so that you can engage them with a view to expediting the according process." Co-Conspirator 4 noted, "As the authorized coordinator, Dr. James Wan would convey our sincere commendation for the leadership in the nation and region with high expectance in full collaboration with [U.N.-Sanctioned Country-1] people in all regards, and wish a fruitful conclusion of business between the two sides."

24. WAN assisted Co-Conspirator 4 in coordinating the planned January 2020 meeting in the PRC. On or about January 10, 2020, WAN sent Co-Conspirator 4 an email with photographs of the passports for two U.N.-Sanctioned Country-1 nationals whom WAN identified as a "Member Of The Board Of Directors And Deputy Director-General of [U.N.-Sanctioned Country-1] Africa Investment Portfolio" and the "Logistic manager [Armed Group-1]."

25. Co-Conspirator 1 and WAN did not plan to participate in the 2020 meeting in the PRC in their individual capacities, but rather in their capacities as representatives of shell companies they created and/or controlled. By early 2020, Co-Conspirator 1 and WAN created and/or controlled at least two shell companies in countries located in the MENA region:

**HSD AND SEALED**

15

a. On or about March 11, 2019, Co-Conspirator 1 sent WAN an email with the subject line of “power of Attorney” and a document from an entity that, according to the document, has an address in U.N.-Sanctioned Country-1 (referred to herein as “CC1 Company-1”). The document states:

Following the meeting of the Board of Directors of [CC1 Company-1] 11/03/2019, the Board members passed the resolution to authorize D r. James Wan, to act on our behalf in all manners relating to Aviation, Oil, and Gas, including the signing of all documents relating to these matters. This authorization is valid until further written notice from [CC1 Company-1].

According to the plain language of the text, the document conveyed to WAN power of attorney over aviation, oil, and gas transactions for CC1 Company-1, which I assess to be one such shell entity used in the criminal scheme.

b. On or about November 7, 2019, Co-Conspirator 1 sent an email to WAN with the subject line “drone jet, and Anti Drone.” Attached to the email was a document on letterhead for an entity with an address in MENA Country-3, ostensibly signed by Co-Conspirator 1 in his capacity as chairman of the board (referred to herein as “CC1 Company-2”), that “authorize[s] Dr. James Wan, to act on our behalf in all manners relating to negotiating an adequate business agreement with Chinese companies, regarding drone jet, and Anti-Drone.”

c. On or about January 10, 2020, WAN wrote Co-Conspirators 1 and 2 asking for the location that the two Armed Group-1 representatives traveling to a meeting in furtherance of the scheme would “apply their visa from and the bank information.” He further asked for the “company name and bank account info”—reflecting WAN’s awareness that one or more of the shell companies were created for the specific purpose of facilitating the transaction with Armed Group-1. The meeting ultimately took place in MENA Country-3.



**HSD AND SEALED**

16

26. Co-Conspirator 4 invited Co-Conspirator 1 in his capacity as “General Director” of “[CC1 Company-2]” of [U.N.-Sanctioned Country-1]. The letter, dated January 16, 2020, invited Co-Conspirator 1 to visit Front Company-1 in Chengdu, PRC “at your convenience before January of 2020 ,for a high level meeting discussing about the technical cooperation.”

27. The investigation has not uncovered evidence suggesting that this above referenced meeting in the PRC occurred as contemplated—likely because of the onset of the COVID-19 pandemic in the PRC during the beginning of 2020.

28. By late January 2020, however, WAN and Co-Conspirators 1 and 2 were attempting to coordinate a meeting to occur in U.N.-Sanctioned Country-1, together with Co-Conspirators 3 and 4. On or about January 21, 2020, WAN wrote Co-Conspirators 1 and 2 an email with the subject “Passports attached,” attaching photographs of Co-Conspirator 1’s PRC passport and WAN’s U.S. passport. Similarly, on or about January 22, 2020, WAN wrote Co-Conspirator 1, “Please confirm me when you plan to meet in [U.N.-Sanctioned Country-1] and your schedule to leave from Montreal. We need to book tickets ASAP.” Attached to the email were photographs of various passports, including the PRC passports of Co-Conspirators 3 and 4 and the U.S. passport of WAN.

29. On or about February 24, 2020, WAN wrote Co-Conspirators 1 and 2, “[MENA Country-2] embassy was informed officially (attached). The official fax sent last night.” The attachment was a document dated February 18, 2020, from the “[U.N.-Sanctioned Country-1] left-behind Office of the People’s Republic of China” indicating that, “in order to promote the needs of [U.N.-Sanctioned Country-1] export projects, [two specified individuals] will go to [U.N.-Sanctioned Country-1] (or a third country) from February 10 to March 10, 2020, to sign an export project agreement with China.”



**HSD AND SEALED**

17

30. As with the planned meeting in the PRC, the investigation has not uncovered evidence demonstrating that the contemplated meeting in U.N.-Sanctioned Country-1 in early 2020 occurred as planned. Notwithstanding the global health crisis, WAN and co-conspirators continued negotiating the arms brokering scheme throughout 2020 and met in MENA Country-3 in late March and early April of 2020.

31. On or about March 12, 2020, WAN wrote Co-Conspirators 1 and 2 about WAN's discussions with individuals in the PRC and included a document containing his recommendations based on these conversations. In the document, WAN characterized PRC Company-1 as a state-owned company and as an official PRC government channel. Indicating that PRC Company-1 "has even more strict rules and procedures to follow," WAN stated that PRC Company-1 is prohibited from dealing directly with U.N.-Sanctioned Country-1 due to a recent United Nations resolution and included a link to the relevant U.N. resolution. Notably, the relevant U.N. resolution called for member states to fully comply with the arms embargo that had been mandated by the U.N. Security Council on U.N.-Sanctioned Country-1 years earlier.

32. In the same document, WAN wrote that PRC Company-1 "can deal with the 'Landing state or company' with closed eyes regarding the actual end users. Accordingly, they require the 'landing company information' to complete the draft of contract and get the approval from the Ministry of Commerce before the meeting that complicate the business." In other words, WAN indicated that PRC Company-1 would not sell its products to end users in U.N.-Sanctioned Country-1 without first obtaining approval from the PRC Ministry of Commerce. WAN concluded the email recommending that Co-Conspirator 1 drop the scheme or use "a third party state or company as a proxy dealing with [PRC Company-1]. I can deal with Chinese team to reduce their percentage to cover the loss." Thus, WAN suggested to Co-

**HSD AND SEALED**

18

Conspirator 1 the use of shell companies located or headquartered outside of U.N.-Sanctioned Country-1 (“a third party state or company as a proxy dealing with [PRC Company-1]”) to shield PRC Company-1 from potential sanctions liability.

33. Accordingly, WAN and Co-Conspirator 1 have created and used multiple shell companies formed in different countries in the MENA region in furtherance of the brokering scheme involving PRC Company-1 and Front Company-1—likely to shield PRC Company-1 and Front Company-1 from liability from sanctions regimes pertaining to U.N.-Sanctioned Country-1. In addition to the shell companies discussed above (CC1 Company-1 and CC1 Company-2), correspondence of WAN and Co-Conspirator 1 repeatedly refers to another shell company under their control which, unlike CC1 Company-1 has a listed address in MENA Country-1, outside of U.N.-Sanctioned Country-1 (referred to herein as “CC1 Company-3”).

34. While the donation of medical equipment to U.N.-Sanctioned Country-1 was ostensibly a goodwill gesture by the PRC government, WAN’s correspondence demonstrates that its true purpose was likely to facilitate an arms transaction between Armed Group-1 and PRC Company-1/Front Company-1 brokered by WAN, and that the PRC government designated members of the conspiracy to arrange the donations.

35. In an April 7, 2020 email, WAN wrote Co-Conspirators 1 and 2 about the medical equipment diplomacy component of the proposed transactions involving drones and drone systems, with the PRC Ministry of Foreign Affairs (“Chinese Foreign Affairs ministry”) authorizing PRC Company-1/Front Company-1 to donate medical equipment as consideration. WAN described the medical equipment that the PRC Ministry of Foreign Affairs was authorizing for donation as follows:



**HSD AND SEALED**

19

1. [Co-Conspirator 1], please provide me an email address other than yours for [PRC Company-1]'s official invitation letter. Just create a new one for [a co-conspirator] for your own access. You can then deliver that letter to him yourself.

2. After a discussion with the Chinese Foreign Affairs ministry, they agree the medical equipment China donating to [U.N.-Sanctioned Country-1] will go through our channel and you are the focal point from the [U.N.-Sanctioned Country-1] side. Therefore, please provide an email address (address to (not yours, but in your own access)), who will receive the medical equipment in [U.N.-Sanctioned Country-1], and where the equipment will be delivered to information to me. All these arrangements will be going through your own arrangement. Please provide me the information ASAP. The donation will be made by the companies ([PRC Company-1] and the manufacturers) involving in the equipment business.

36. On or about April 7, 2020, WAN and Co-Conspirator 3 corresponded about a formal letter from PRC Company-1 with an official stamp indicating that members of Co-Conspirator 1 and WAN's team should meet in the capital city of MENA Country-1 to finalize the contract. This letter was ultimately dated and issued on April 9, 2020. The letter stated, "The high level officer of the Chinese Embassy in [MENA Country-1] will participate the signing ceremony on behalf of Chinese central government." The letter also included a proposed end use certificate stating that the products, which I assess refers to the NGECS, should remain in MENA Country-1 and be only used for "civil end uses," such as medical services, emergency communication, and monitoring the environment and land use—notwithstanding the obvious military applications of the drones and drone systems. WAN forwarded this correspondence to Co-Conspirators 1 and 2.

37. On or about May 13, 2020, WAN replied to an email about "establishing the business relations between [PRC Company-1] and [CC1 Company-3]." WAN emailed Co-Conspirator 1, requesting that Co-Conspirator 1 sign an attached "Contract of Intend" and send it to Co-Conspirator 4 and WAN himself. The draft contract, which pertained to the sale of the

**HSD AND SEALED**

20

NGECS system, reflects execution dates in 2020 and 2021 with the co-conspirators' shell company CC1 Company-3 as the purchaser and end user. Co-Conspirator 1 was referenced in the document as the legal representative of CC1 Company-3. I assess that CC1 Company-3 was not the ultimate intended end user, but rather that Armed Group-1 was the actual intended end user.

38. The draft contract included language specifying that PRC Company-1 and Front Company-1 would be the manufacturers, while the general contractor would be a U.K. Company ("U.K. Company-2"). Based on information obtained during the investigation, I assess that U.K. Company-2 is another shell entity linked to the co-conspirators; its name is similar to that of the U.K. Company-1 controlled by Co-Conspirator 6 referenced above. Notably, the draft contract provided, "All the parties involved in the contract should strictly abide by the laws, regulations, and resolutions formulated by the U.N., international community and related governments and authorities." As noted herein, providing military equipment to end users in U.N.-Sanctioned Country-1, including drones with attack capabilities, would violate U.N. mandated sanctions measures. On or about May 15, 2020, a PRC Company-1 employee sent WAN and Co-Conspirator 1 proposed revisions to a contract for the NGECS system that Co-Conspirator 1 had signed.

39. On March 18, 2021, WAN wrote an email attaching a letter dated March 18, 2021 from the U.N.-Sanctioned Country-1 "Minister of State for Cabinet Affairs" to the "Cabinet Minister, National Health Commission, People's Republic of China," seeking the PRC government's "assistance in the procurement of the [COVID-19] vaccine." As discussed above, the provision of medical equipment and supplies from the PRC government, including PRC-manufactured COVID-19 vaccines, has been a component of the co-conspirators' brokering activities involving military drones and drone systems.



**HSD AND SEALED**

21

40. On March 27, 2021, WAN sent to himself an email with a draft consultancy agreement between, among other parties, PRC Subsidiary-1 and CC1 Company-3. The agreement called for the provision of a “New Generation Emergency Communication System [NGECS] in the Middle East . . . and North Africa . . . region” for no less than \$500 million annually.

Arms Brokering Activities in Other Jurisdictions

41. In 2021, the relationship between WAN and Co-Conspirator 1, on the one hand, and PRC Company-1 and Front Company-1, on the other hand, expanded to MENA Country-2 and other jurisdictions in the Middle East and Northern Africa.

42. On or about February 17, 2021, WAN forwarded an unsigned power of attorney document indicating that WAN and Co-Conspirators 1 and 5 were “the sole agent representatives on behalf of [PRC Subsidiary-1] & [Front Company-1] in Arica and MENA regions to conduct the negotiations and check the related contracts and agreements under the New Generation of Emergency Communication System Projects [NGECS].” On February 23, 2021, WAN wrote an email attaching a power of attorney document bearing Co-Conspirator 4’s signature indicating that WAN and Co-Conspirators 1 and 5 are “the sole agent representatives on behalf of [PRC Subsidiary-1] & [Front Company-1] in Middle East and North Africa (MENA) region to conduct the negotiations and check the related contracts and agreements under the project for New Generation of Emergency Communication System [NGECS].”

43. On or about March 4, 2021, a PRC Company-1 employee wrote to Co-Conspirator-5 and copied WAN and Co-Conspirators 1 and 3 to introduce them to a PRC Company-1 employee from PRC Subsidiary-1, described as the individual who is going to “coordinate with you for the NGECS Project in MENA region.”



**HSD AND SEALED**

22

44. On or about May 4, 2021, WAN and Co-Conspirator 5 (the principal of MENA Entity-1) participated in a videoconference. Notes of the meeting, found in Co-Conspirator 5's electronic storage account, reflect the following, in relevant part:

J [WAN] explained that due to [PRC Company-1] having governmental functionalities in China, it is infeasible to put profit-sharing business notions into an official agreement with [PRC Company-1].

J [WAN] presented a business model endorsed by [PRC Company-1] and [Front Company-1], meeting the profit-oriented business partnership. To the intended project, the New Generation Emergency Communication System (NGECS), the total amount of the main project size is 1 billion USD, which will be signed between the customer and [PRC Company-1] at a designated Chinese embassy. In the same main contract signing event, [PRC Company-1] will sign the subcontract with [MENA Entity-1] with a total amount of 190M USD out of the main project monetary amount (1 billion USD), which will be treated as the profit (commission) of the contracted project (NGECS). Among the 190M (the Amount), the [MENA Entity-1] owns 75% (representing 142.5M USD) of the Amount, and [U.K. Company-1] owns the rest of 25% (representing 47.5M USD) of the Amount.

[Co-Conspirator 5] supported [PRC Company-1/Front Company-1] proposed business model and suggested both parties need to have an official profit-sharing agreement between [MENA Entity-1] and [Front Company-1].

....  
J [WAN] confirmed [PRC Company-1] and [Front Company-1] are authorizing him to attend technical and business meetings when needed and make necessary decisions.

45. On or about May 12, 2021, WAN and Co-Conspirator 1 were copied on an email from Co-Conspirator 4 to Co-Conspirator 5—the principal of MENA Entity-1—and indicated that Front Company-1 was interested in selling NGECS to the government of MENA Country-2 and simultaneously establishing a joint venture for systems with civilian and military capabilities where “initial parties shall be a [MENA Country-2] local company with [Front Company-1/PRC Company-1] consortium in the early stage to form a JV company and gradually spread to the Middle East and Africa.”

**HSD AND SEALED**

23

46. WAN and his co-conspirators appeared to take steps in furtherance of this proposal described above. On or about June 7, 2021, WAN wrote to Co-Conspirators 3 and 4, “I updated the list of names received this email and add [MENA Country-1] to the last paragraph. This deal will be happening in [MENA Country-1] with the funding support from [MENA Country-2] so [Co-Conspirator 5] asked the [MENA Country-1] government must be mentioned in the email.” The email included an attachment addressed to executives at a defense company located in MENA Country-2, referred to herein as “MENA Defense Contractor-1.” The attachment was written in Co-Conspirator 4’s name and revised by WAN. The document outlined a plan for a joint venture between Front Company-1 and MENA Defense Contractor-1 regarding drone and anti-drone systems, including transferring Front Company-1’s technology and expertise to MENA Country-1 and MENA Country-2 and establishing manufacturing for PRC Company-1/Front Company-1 drone and anti-drone systems in MENA Country-1 and MENA Country-2. The attachment stated that “the [joint venture] shall involve [MENA Country-2] and [MENA Country-1] companies with [Front Company-1/PRC Company-1] consortium in the early stage and gradually spread to the Middle East and Africa.”

#### The 2021 Meeting

47. Documents uncovered in the investigation reflect that the co-conspirators met in the Middle East during the late summer of 2021.

48. On August 28, 2021, WAN wrote Co-Conspirator 3 an email with the subject “Delegations”—possibly a reference to the forthcoming meeting in the Middle East. Attached to the email was a document reflecting the representatives of PRC Company-1, Front Company-1, and MENA Entity-1 “as the Exclusive Agency of [PRC Company-1] and [Front Company-1].” Co-Conspirator 5 (“Chairman”) and WAN (“Consultant”) were the listed



**HSD AND SEALED**

24

representatives of MENA Entity-1, and Co-Conspirator 3 (“Senior Vice President”) was one of the listed representatives of Front Company-1. Notably, the document included WAN’s “Nationality” as “U.S.” and indicated WAN’s passport number and expiration date. On the same date, WAN wrote Co-Conspirator 1 an email attaching copies of Co-Conspirator 5 and WAN’s passports.

49. Also on August 28, 2021, WAN wrote Co-Conspirator 3 an email with suggested language for Co-Conspirator 4’s response to an invitation letter pertaining to a forthcoming meeting:

Thank you for the email. I am truly pleased to accept your invitation to visit your esteemed company in [MENA Country-2]. Indeed, [Front Company-1] and our partners are expecting to open full discussion with [MENA Defense Contractor-1] regarding our intended joint venture in such as, but not limited to, production, product research & development, and in-depth knowledge and technology transfer. [Front Company-1] fully endorses this engagement with [MENA Defense Contractor-1] and [MENA Entity-1] with the expectation of signing an MOU for such important cooperation.

Please kindly find out the mixed delegation list of [PRC Company-1], [Front Company-1], and [MENA Entity-1].

Best wishes,

[Co-Conspirator 4]  
Chairman of [Front Company-1], China

50. The investigation has obtained a photograph of WAN, Co-Conspirator 5, who is a citizen of MENA Country-1, and other two individuals all posing for a photo on the premises of a hotel. In the background of the photograph are large, distinctive and well-known monuments and tourist attractions that I assess to be located in MENA Country-1. WAN emailed the photograph to himself on or about August 30, 2021 and the naming convention of the photo’s file indicates that it was likely taken on the same date.

**HSD AND SEALED**

25

51. Following this meeting, the co-conspirators have continued planning transactions involving the sale of PRC Company-1/Front Company-1 drones and drone systems to governments in the MENA region. On or about October 27, 2021, Co-Conspirator 4 wrote to Co-Conspirator 5 copying WAN, detailing the pricing of PRC Company-1's Wing Loong II drone and its components, a video produced by PRC Company-1 demonstrating the attack capabilities of the Wing Loong II, and a document listing the technical specifications of the NGECS, which included images of the Wing Loong II equipped with weapons and detailed the targeting and payload specifications of NGECS components. The pricing document was watermarked "[Front Company-1] and [PRC Company-1]."

52. On or about October 29, 2021, Co-Conspirator 5, sent an email to WAN and Co-Conspirator 4 attaching a document from an investment group in MENA Country-2 that advertised its ownership by a politically prominent family in MENA Country-2 ("MENA Investment Group-1") that sought business with MENA Entity-1. The attached document from MENA Investment Group-1 contained a request for a quote for the Wing Loong II drone. On or about November 15, 2021, Co-Conspirator 4 forwarded WAN a signed agreement between MENA Investment Group-1, Front Company-1, and MENA Entity-1, designating MENA Investment Group-1 as Subsidiary 1's exclusive agent in MENA Country-2 and other MENA countries, and MENA Entity-1 as the regional distributor for Front Company-1.

The 2021 Defense Expo

53. As part of his brokering activities, WAN participated as an exhibitor at the 2021 iteration of a biannual trade show for arms manufacturers and defense contractors in MENA Country-1 that was supported by the armed forces of MENA Country-1 (the "Defense Expo"). On or about November 3, 2021, WAN received an email thanking him for registering



**HSD AND SEALED**

26

as an exhibitor at the Defense Expo scheduled to be held from November 29 to December 3, 2021. According to the Defense Expo's website, Front Company-1 was an exhibitor at the Defense Expo in 2021. On or about September 14, 2021, a businessman from MENA Country-1 who has corresponded with WAN about weapons deals emailed Co-Conspirator 4 and WAN asking Front Company-1 to attend the Defense Expo. The MENA Country-1 businessman noted:

As we would like you to know the importance of this EXPO. From our point of view, we must to participate in such Expo as exhibitors due to the attendance of defense Ministers, Chiefs of War's Staff and the official's decision makers for Middle East, Africa, Arabian Gulf and some other countries. my team and I are honored to supporting you to participate of such Expo especially that there is a lot of constraints and limitations for applicants (Expo organizer did not accept all of the applicant).

54. Co-Conspirator 4 solicited business from an entity based in a fourth MENA country ("MENA Country-4") during the Defense Expo, and on or about December 5, 2021, Co-Conspirator 4 forwarded WAN a message from a representative of a defense firm located in MENA Country-4 ("MENA Defense Contractor-2"):

Let me start by thanking you for the time you gave us last week during your visit at [the Defense Expo] in [the capital city of MENA Country-1], we absolutely enjoyed it.

As we have discussed, [MENA Defense Contractor-2] is a purely [MENA Country-4] based company with a reputable profile of dealing with the entire [MENA Country-4] Military & Security entities and Subsidiary companies. As we have explained the interest to participate in the upcoming Military Exhibition . . . next March in [the capital city of MENA Country-4] which will guide us to build solid partnerships with new reputable partners. Hence, it would be greatly appreciated if we are able to discuss our cooperation in this regard, likewise appreciate discussing cooperating in the Business in [the capital city of MENA Country-4] using our solid network and references as well. Therefore, kindly feel free to share your company's profile and your positive thoughts in the mentioned cooperation above. Looking forward to hearing from your side.

**HSD AND SEALED**

27

According to open-source materials, MENA Defense Contractor-2 sells military supplies, software, and security and military training consulting services.

55. Notably, WAN received this email from Co-Conspirator 4 after he was authorized by Co-Conspirator 4 to act as one of “the sole agent representatives on behalf of [PRC Subsidiary-1] & [Front Company-1] in Middle East and North Africa (MENA) region to conduct the negotiations and check the related contracts and agreements under the project for New Generation of Emergency Communication System.” See supra Paragraph 42.

Brokering Activities Continue in 2022

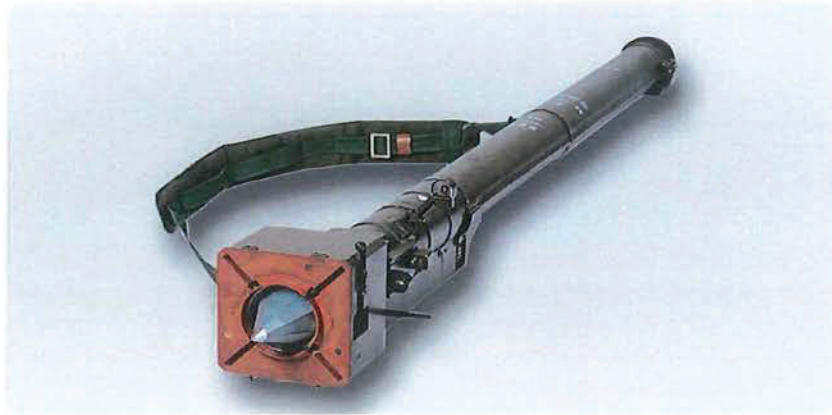
56. In 2022, WAN has continued his brokering activities in the MENA region. In January and February 2022, WAN sent himself a series of brochures for various weapons or weapons systems, which based on the facts set forth in this affidavit, I assess he is likely seeking to sell to third parties. These brochures include:

a. The “FN-16 Portable Air Defense Missile System,” also referred to as the “FN-16 MANPAD,” which is a “missile [that] employs IR and UV dual color homing guidance seeker, the combination of laser proximity fuse and impact fuse” and “has all-direction attack, anti-infrared decoy and ‘fire-and-forget’ capabilities,” used to “intercept various types of attack helicopter, fixed-wing aircraft, cruise missile and UAV.” Based on my training and experience, I assess that the “FN-16 Portable Air Defense Missile System” constitutes “an explosive or incendiary rocket or missile that is guided by any system designed to enable the rocket or missile to seek or proceed toward energy radiated or reflected from an aircraft or toward an image locating an aircraft; or otherwise direct or guide the rocket or missile to an aircraft” under 18 U.S.C. § 2332g(a)(1)(A). The “FN-16 MANPAD” is depicted below:

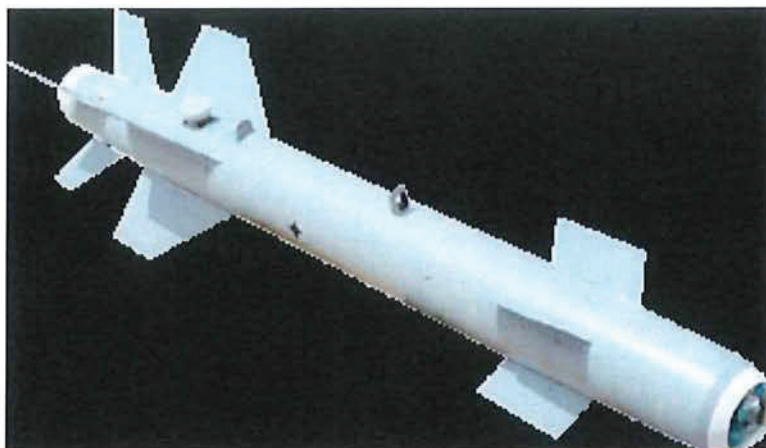


**HSD AND SEALED**

28



b. The “YZ-200 Series Laser Guided Bomb,” which is “an advanced precision guided bomb, used for air-to-surface attacks of a variety of targets,” featuring a 30 kilogram penetration blast or tandem shaped-charge blast fragmentation warhead with “GPS/INS guidance and a semi-active laser seeker” and “anti-jamming capability.” Notably, this brochure was marked with the name of a PRC state-owned defense company not owned by PRC Company-1. The “YZ-200 Series Laser Guided Bomb” is depicted below:



c. The “AR-2 Air-to-ground Missile” that features a 4.5 kilogram “fragmentation-blast warhead” with a range of 1.5 to 8 kilometers and is described in the brochure as “designed specifically for UAV to perform attacking mission in military operation,” depicted below:

**HSD AND SEALED**

29



d. The “CM-502KG Short-Range Air-to-Surface Missile Weapon System . . . applicable to medium-to-large sized UAV or aircraft . . . designed to meet the demand of precisely striking stationary or mobile tactical targets, such as missile launching site, parking aircraft, armored vehicle and small sized vessel,” with an 11 kilogram “semi-armor piercing warhead / blast-fragmentation warhead,” with a maximum range of 25 kilometers, depicted below:



57. And the “Z-AMP-LT UAS” unmanned aerial vehicle with a maximum range of 2500 kilometers compatible with a “variety of payloads and weapons” which “can be equipped to conduct missions such as border patrol, coastline patrol, electronic countermeasures, intelligence, surveillance and reconnaissance (ISR) and air-to-ground precision strike.”



**HSD AND SEALED**

30

According to product specifications that WAN sent in February 2022 in a document titled “Large-UAV-Technical-Specification”, the “Z-AMP-LT UAS” is compatible with air-to-surface weapons systems, including semi-armor piercing warheads, blast fragmentation warheads, laser guided bombs, and laser guided missiles. The specifications document highlights the “major performance” for some of these missiles is attacking fixed targets, including “people” and “light vehicles.” A promotional video WAN sent himself that features Front Company-1’s logo includes visual depictions of “Air Target Tracking,” among other capabilities. Images of the drone from the brochure with weapons affixed are depicted below:



**HSD AND SEALED**

31



Fig. 6- 3 Schematic Diagram of Z-AMP-LT UAV with Full External Stores

58. During early 2022, WAN sent to himself various draft agreements or quotations for the provision of military items. One draft contract was between Front Company-1 and a party to be named—likely one of the co-conspirators’ shell companies. The draft calls for the payment of \$333,113,072 in return for provision of the NGECS system. An invoice for \$147,607,724 contemplates the sale of, among other items, an NGECS system and an “Anti UAV System” with a “Detection & Suppression Payload.” Another “Quotation” contemplates that an end user would purchase the following items in the following amounts:

**HSD AND SEALED**

32

**Quotation**

Unit: USD

S/N	Items	Unit	Qty.	Unit Price	Remarks
<b>Air-to-surface Weapon system</b>					
I	Weapon				
1	CM-502KG				
(1)	CM-502KG missile (laser)- semi-armor piercing warhead	pc	More than 500	124,193.55	The main specifications of AR-1 are similar with that of CM-502KG, they are interchangeable. The comparison of specifications refers to Annex 1 in detail.
(2)	CM-502KG missile (IR)- semi-armor piercing warhead	pc	More than 500	158,064.52	
(3)	CM-502KG missile (TV)- semi-armor piercing warhead	pc	More than 500	141,935.48	
(4)	CM-502KG missile (laser)- blast-fragmentation warhead	pc	More than 500	130,645.16	
(5)	CM-502KG missile (IR)- blast-fragmentation warhead	pc	More than 500	164,516.13	
(6)	CM-502KG missile (TV)- blast-fragmentation warhead	pc	More than 500	146,774.19	
2	FT-9 bomb (laser)	pc	More than 500	75,806.45	The main specifications of YZ-212D are similar with that of FT-9, they are interchangeable. The comparison of specifications refers to Annex 2 in detail.
3	FT-8C missile (laser)	pc	More than 500	80,645.16	The main specifications of AR-2 are similar with that of FT-8C, they are interchangeable. The comparison of specifications refers to Annex 3 in detail.
II	Support Equipment				
1	CM-502 daily test equipment	set		448,387.10	Including missile tester, initiating explosive device detector and missile supporting vehicle.
2	FT series portable weapon tester	set		161,290.32	
3	General-purpose adapter	set		4,838.71	
4	General-purpose pylon	set		20,967.74	For both CM-502KG and FT-9
5	FT-8C launcher	set		66,129.03	Special for FT-8C
<b>Surface-to-air Weapon system</b>					
1	Surface-to-air Weapon	set	More than 500	260,000	One set Surface-to-air Weapon includes 1 launcher, 2 missiles and 4 ground support energy
	Note: 1. This quotation is the factory price, excluding taxes, transportation and relevant exporting fees; 2. Relevant training fees are not included in this quotation; 3. The exchange rate between RMB and USD is 6.2.				

Notably, the quotation indicates a price for the purchase of “[m]ore than 500” “Surface-to-air Weapon[s],” described as “One set Surface-to-air Weapon includes 1 launcher, 2 missiles and 4 ground support energy.”

59. Another document WAN forwarded to himself in early 2022 was a document titled “Reply on Client’s Inquiries” that metadata indicates was last modified by WAN. This document includes narrative responses to various questions regarding the military



HSD AND SEALED

33

drone systems WAN has been selling. In relevant part, WAN described the NGECS system as follows: “various equipment, device, weapon and sea/land/air motorized platform (UAV is the air motorized platform) are integrated as an operation system.” The document further stated that “[t]here are there types UAV described in the company file” and proceeded to identify “Large-scale UAV” “Middle-scale UAV” and “Small-scale UAV,” some of which had capacity for substantial payloads, including the “Large-scale UAVs” “*Winglong 2*, 20.5m wingspan, 480kg payload and 20h endurance” and “*Z-AMP-LT*, 20.5m wingspan, 480kg payload and 35h endurance.” The document also included the following responses to the questions excerpted below:

Question: 5. The report mentioned that the air-to-air missile (PL10E) is 3.69 m long, and this is too big for the size of the plane, so we hope that you will send a picture of the plane equipped with this missile?

Answer: . . . We will develop a series of cost-effective alternative missiles to replace the PL10E, which may be suitable for the large and middle UAVs.

Question: 7. Can this UAV intercept hostile UAVs such as the Iranian UAV (Ababeel-T) while in flight, using the PL10E missile?

Answer: PL10E is the fourth generation air to air combat missile with high performance. It is equipped infrared imaging guidance system an has high accuracy for UAV target.

Question: 8. The profile mentions that the air-to-air missile (PL10E) is guided by infrared radiation. How is the target detected in the air and locked to it, so that the UAV then launches the missile to destroy it... Are there any restrictions for this process?

Answer: The PL10E is guided by infrared imaging, which will detect and lock the air targe based on infrared imagery (targe shape) rather than infrared point source. This guidance system can obtain much



**HSD AND SEALED**

34

more information from the target and has strong anti-interference and high accuracy in the guidance. Also, it has the ability to distinguish multiple targets. So, it has a high performance in air combat.

Based on my training and experience, I assess that the air-to-air missiles and anti-UAV systems discussed in this document meet the definition of items addressed by 18 U.S.C. § 2332g.

60. Correspondence from 2022 further corroborates that MENA Entity-1 and MENA Investment Group-1 are involved in furtherance of the scheme to sell PRC Company-1/Front Company-1 military drone systems. On or about February 13, 2022, Co-Conspirator 4 wrote Co-Conspirator 5 and WAN an email with the following language:

This email is to confirm that [Front Company-1], a government owned company, has been officially authorized and certified by the Chinese government to work with licensed agencies, namely [PRC Company-1] and [a separate PRC-based defense manufacturer], to carry out the intended business with [MENA Entity-1] and [MENA Investment Group-1] of [MENA Country-2].

Best regards,

[Co-Conspirator 4]  
Chairman of [Front Company-1]

61. On or about April 5, 2022, Co-Conspirator 4 wrote an email to a MENA Investment Group-1 business email account with the subject "Performance review of [MENA Investment Group-1]." WAN forwarded himself the email on or about April 6, 2022, further corroborating that MENA Investment Group-1 is involved in the brokering scheme.

62. Another MENA Country-2 company used by the co-conspirators to facilitate the sale of PRC Company-1/Front Company-1 military drone systems is MENA Entity-2. On or about April 11, 2022, Co-Conspirator 4 forwarded a signed consultancy services agreement between Front Company-1 and MENA Entity-2. According to the agreement,

**HSD AND SEALED**

35

MENA Entity-2, agrees to market NGECS for sale in the Middle East and Africa region, and will enjoy “5% . . . of the Final Value of any business, products, contracts, or supply orders.”

63. On or about April 28, 2022, while WAN was in Queens County in the Eastern District of New York, Co-Conspirator 4 forwarded WAN a general contract between Front Company-1 and a party to be named—likely one of the co-conspirators’ shell companies. The contract, worth \$1.54 billion, called for the provision of an NGECS system, including a “large air platform” and “airport protection subsystem, middle air platform and small air platform system,” which appear to refer to the “large-scale” “middle-scale” and “small-scale” UAVs discussed in WAN’s “Reply on Client’s Inquiries” document that are components of NGECS and some of which are capable of handling air-to-air and air-to-ground explosive weapons, including missiles. See supra Paragraph 59. Based on my training and experience, I assess that the air-to-air missiles capable of being attached to the “large air platform” and “middle air platform” described in the contract sent by Co-Conspirator 4 constitute a “device designed or intended to launch or guide a rocket or missile” under 18 U.S.C. § 2332g(a)(1)(B).

64. On or about June 25, 2022, WAN drove into the United States from Canada and was interviewed at the border by officers of U.S. Customs and Border Protection. During secondary inspection, officers determined that WAN had recently traveled to MENA Country-1. WAN indicated that he had traveled to MENA Country-1 for business regarding an “auto retractable syringe” project with a particular medical equipment company that he identified. Notably, WAN refused to provide the name of his contact in MENA Country-1 but described the contact as “a very important political figure in the [MENA Country-1] government.”



**HSD AND SEALED**

36

65. The investigation has uncovered evidence suggesting that WAN has benefitted financially from the scheme. At least one financial institution has recently questioned WAN about his unexplained wealth. On or about July 18, 2022, a financial planner at a Canadian financial institution contacted WAN, seeking to discuss “the significant amount deposited into your account. It is a question of safety but also of profitability.”

66. Similarly, on or about November 22, 2022, WAN wrote an email to an individual in Canada: “Since December, I will be traveling to China, Taiwan, Africa, middle east and south America until settled my family in China in May or June.” In sum and substance, WAN stated that he was traveling to the MENA region in December 2022 to finalize terms of a \$150 billion transaction involving importing crude oil to the PRC, for which he would obtain shares worth “10 M a month” beginning in February 2023. WAN indicated, “My business is finalized and they are finalizing the payment method and banking process now, waiting for signing ceremony in December as all legal processes were completed.” In the same email correspondence, WAN wrote that he removed close friends on a specified electronic messaging platform “to protect you for in case any government is watching,” which may indicate a growing concern that his activities are subject to law enforcement scrutiny. Notably, electronic communications obtained by the government reflect that WAN was booked on a one-way flight departing December 20, 2022, from Montreal, Canada, and arriving in a fifth country located in the MENA region (“MENA Country-5”). Electronic communications further reflect that WAN was subsequently booked on a one-way ticket on a flight departing December 30, 2022, from MENA Country-5 and arriving in MENA Country-1. Electronic records for two separate email accounts used by WAN further reflect that on or about December 30 and 31, 2022, WAN accessed those email accounts through Internet Protocol addresses that resolve to Internet service

**HSD AND SEALED**

37

providers located in MENA Country-1, indicating that WAN was likely located in MENA Country-1 at the time of access.

WHEREFORE, your deponent respectfully requests that an arrest warrant issue so that the defendant KUANG CHI WAN, also known as “James Wan,” may be dealt with according to law.

REQUEST FOR SEALING

67. I request that the Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the Amended Complaint and arrest warrant, with the exception that the Amended Complaint and arrest warrant be unsealed for the limited purpose of disclosing the existence of, or disseminating, the Amended Complaint and/or arrest warrant to relevant United States, foreign, or intergovernmental authorities, at the discretion of the United States and in connection with efforts to prosecute the defendant or to secure the defendant’s arrest, extradition or expulsion. Based upon my training and experience, premature disclosure of the contents of the Amended Complaint and related documents will



**HSD AND SEALED**

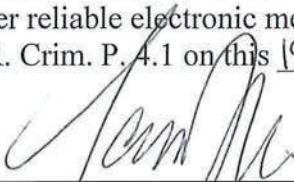
38

seriously jeopardize the investigation, including by giving the defendant an opportunity to flee from prosecution, destroy or tamper with evidence and change patterns of behavior.



GARY PHILLIPS  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone  
or other reliable electronic means pursuant to  
Fed. R. Crim. P. 4.1 on this 19<sup>TH</sup> day of January, 2023



THE HONORABLE ~~VERA M. SCANLON~~ JAMES R. CHO  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK